IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	
	)	**No. 18 CR 789**
v.	)	
	)	**Hon. Gary Feinerman**
DENY MITROVICH,	)	
	)	
Defendants.	)	

MOTION TO COMPEL DISCOVERY

Now comes the defendant, Deny Mitrovich, by and through his undersigned attorney, and pursuant to Federal Rule of Criminal Procedure 16, *Brady v. Maryland*, 373 U.S. 83 (1963), and its progeny, respectfully moves this Honorable Court to compel the government to comply with its discovery obligations and produce the specific discovery requested, to wit: 1) any and all communications between the government and Queensland Police Services (QPS)/Department of Internal Affairs (DIA) and 2) information regarding the software used to unlawfully seize Mr. Mitrovich's IP address. In support, the following is offered:

Relevant Factual Background[1]

The FBI, along with other law enforcement agencies, were investigating an internet-based website whose alleged primary purpose was the advertisement and distribution of child pornography. That website is now known as "The Love Zone"

[1] All factual assertion are taken from the application and affidavit for a search warrant *In the Matter of the Search of [Mr. Mitrovich's apartment],* Case No. 15M275 and from FBI reported dated 3/27/2015 (MITRO_00001-00004). Both documents can be provided to this Court, should such be necessary.

(TLZ). While TLZ was still operational, it was specifically designed to facilitate anonymous communication over the internet so long as the potential user installed publicly available computer software. This is known as the "The Onion Router" or "Tor" network. The "Tor" network allows users to search the "dark web". During the FBI's undercover investigation through a previously seized account of TLZ, was the profile page of a user named "cyberguy" who had originally registered for an account on TLZ on or about August 3, 2019 and became a "Full Member" of TLZ on or about August 11, 2014.

In mid-2014, the FBI obtained the ability to identify IP addresses associated with certain users of TorChat and certain hidden services. A review of the IP addresses associated with TLZ revealed that TLZ was hosted in The Netherlands, with the head administrator residing in Australia. Pursuant to this information obtained by the FBI, in late 2014, the QPS/DIA seized control of TLZ and operated the website for a period of time in an undercover capacity.

The QPS/DIA were investigating TLZ at the same time as the FBI. In June 2014, the QPS/DIA arrested a user of TLZ and subsequently contained consent to assume the user's account on TLZ and took over operation of the account. Pursuant to his arrest, the user also provided the QPS/DIA with his backup copy of TLZ which contained dated revealing information on users' accounts, profiles posts, and private messages. One of the accounts was "cyberguy". A copy of this backup, along with copies of subsequently contained backups were provided to the FBI. TLZ was controlled by QPS/DIA from TLZ from September 2014 through December 2014.

In early November 2014, a hyperlink to a file within a forum on TLZ was uploaded that was accessibly only to members of TLZ. The hyperlink was advertised as a preview of a child pornography website with streaming video. When a member of TLZ clicked on that hyperlink, the member was allegedly advised that the user was attempting to open a video file from an external website. If the member chose to open the file, a video file containing images of child pornography began to play. This allowed QPS/DIA to capture and record the IP address of the user accessing the file. This was able to be accomplished, despite the members using a "Tor" network, because the hyperlink was able to be configured wherein the video file opened an Internet connection outside of the "Tor" network. This allowed the capture of the user's actual IP address, as well as a session identifier to tie the IP address to the activity of a particular TLZ user account. Users were not warned that upon clicking the hyperlink, they would be rerouted off of the "Tor" network and onto an open Internet connection. On November 11, 2014, one of the users to click the hyperlink was "cyberguy". This allowed the capture of his IP address.

In December 2014, the FBI, using the IP address associated with "cyberguy", obtained records from Comcast regarding the account holder for that IP address at the time the hyperlink was clicked, as well as the address associated with the IP address. A review of Illinois Secretary of State records and law enforcement databases showed that Mr. Mitrovich, along with his wife, resided at the address associated with the seized IP address. Using this information, in May 2015, the government was able to obtain a search warrant for the physical address associated

with "cyberguy". Through the use of the search warrant, the government was able to search Mr. Mitrovich's house and computers which allegedly revealed child pornography videos and photographs on a computer and external hard drive located in the house. Mr. Mitrovich was subsequently indicted on allegation of possession of child pornography.

On September 16, 2019, Mr. Mitrovich sent the government a discovery requesting the following:

1. A copy of the "note with passwords" that was allegedly found in the top left drawer of the computer desk;

2. A copy of the MCCU user report for "cyberguy" that is referenced on MITRO_00003;

3. Reports generated by QPS/DIA and provided to MCCU as referenced on MITRO_00002;

4. Any and all discovery relating to the FBI and MCCU "ability to identify IP addressed associated with certain users of TorChat and certain hidden services" as referenced on MITRO_00001. This includes but not limited to the name of the software used, any and all manuals related to the software, logs kept throughout course of investigation, all training materials, including but not limited to training records, certification records, training standards, and training manuals, all policies and procedures regarding use of this software, names and curriculum vitae of any and all individuals who operated, and any and all records utilized by FBI and MCCU during course of this investigation as it relates to this software; and,

5. Any and all communications between the FBI/MCCU and QPS and DIA throughout Operation Downfall II, as referenced on MITRO_00001-00002, including email communications, letters, and any and all attachments including the reports generated of each user through TLZ sting that were "generated by QPS/DIA and provided to the MCCU for further identification."

In response to this request, the government forwarded request number 1 to counsel for Mr. Mitrovich. Additionally, the government allowed the undersigned to review requested items numbered 2 and 3. As to the remaining discovery requests, the government responded:

> We will not produce materials in response to #4 because that quoted reference pertains to Operation Downfall Part 1 and is not related to Mitrovich, whose IP address was not obtained in that manner. (His IP address was obtained in Operation Downfall Part 2, when QPS/DIA was operating TLZ in an undercover capacity.)
>
> We will also not produce any materials in response to #5. Even assuming the US government were accountable for the conduct of QPS/DIA (which we dispute), the investigative use of a URL to reveal Mitrovich's true IP address could not have violated the fourth amendment. Among other reasons, Mitrovich had no reasonable expectation of privacy regarding his true IP address when he clicked the URL on TLZ. As a result, discovery pertaining to the relationship between the US and QPS/DIA is not material to the defense, or otherwise discoverable.

The undersigned later clarified to the government that in regard to request number 4, he was also referencing the software used to redirect users from the "Tor" network to the open Internet. The government still refused. This motion follows.

Legal Standard

It has been long established that the government is required to disclose all evidence material to the preparation of a defense and all potentially exculpatory evidence, regardless of whether they believe it to be exculpatory or not. "One of the central tenets of our criminal law jurisprudence is the prosecution's affirmative duty to disclose evidence favorable to a defendant and material either to the issue of

guilt or to the issue of punishment." *United States v. Gonzales*, 93 F.3d 311, 315 (7th Cir. 1996).

"In the pretrial context, 'the government is obligated to disclose all evidence relating to guilt or punishment which might reasonably be considered favorable to the defendant's case,' with doubt as to usefulness resolved in favor of disclosure." *United States v. Peitz*, 2002 WL 226865, at *3 (N.D. Ill. Feb 14 2002); *quoting United States v. Sudikoff*, 36 F. Supp. 2d 1196, 1199 (C.D. Cal. 1999); *see also United States v. Carter*, 313 F. Supp. 2d 921, 925 (E.D. Wis. 2004); *United States v. Siegfried*, 2000 WL 988164, *1 (N.D. Ill. July 18, 2000)("The fact that denial of discovery might ultimately turn out on appeal not to have prejudiced the defendant or to have constituted an abuse of discretion is not a compelling reason for at trial court not to order the discovery in the first place.").

Additionally, Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure requires the government to provide defendants with documents or other tangible objects within its custody, possession or control that are "material to the preparation of the defendant's defense." To be material, the discovery sought must "significantly help in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment and rebuttal." *United States v. Gaddis*, 877 F.2d 605, 611 (7th Cir. 1989). "Rule 16 materiality has been defined as evidence that would 'enable the accused to substantially alter the quantum of proof in his favor.'" *United States v. Peitz*, 2002 WL 31101681, at *3 (N.D. Ill. Sept 20, 2002); *quoting United States v. Orzechowski*, 547 F.2d 978, 984 (7th Cir. 1976).

"The language and spirit of [Rule 16] are designed to provide a criminal defendant, in the interest of fairness, the widest possible opportunity to inspect and receive such materials in the possession of the government as may aid him in presenting his side of the case." *United States v. Poindexter*, 727 F.Supp.1470, 1473 (D.D.C. 1989). Documents are "material" if they "would have significantly helped in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *United States v. Gaddis*, 877 F.2d 605, 611 (7th Cir. 1989). Both inculpatory and exculpatory evidence must be produced under Rule 16 as "even inculpatory materials may alter the proof in the defendant's favor by helping to prepare a defense or investigation." *Peitz*, 2002 WL 31101681, at *3.

Discovery matters in a criminal case is within the sound discretion of the trial court. *United States v. Bastanipour*, 697 F.2d 170, 175 (7th Cir. 1982). The defendant bears the burden to "make at least prima facie showing that the requested items are material to his defense." *United States v. Thompson*, 944 F.2d 1331, 1342 (7th Cir. 1991). A defendant cannot rely on "general descriptions or conclusory arguments" and must "convincingly explain how specific documents will significantly help him uncover admissible evidence, prepare witnesses, or corroborate, impeach or rebut testimony." *United States v. Caputo*, 373 F.Supp.2d 789, 793 (N.D. Ill. 2005).

The Ninth Circuit has recently addressed discovery material needed for a suppression hearing on the issues of unconstitutional searches and seizures. *See*

United States v. Soto-Zuniga, 837 F.3d 992 (9th Cir. 2016). There, *Soto-Zuniga* was seized at a road checkpoint and argued that his seizure violated the Fourth Amendment. *Id.* at 999. *Soto-Zuniga* sought to compel the government to disclose search and arrest statistics from the checkpoint where the seizure occurred; the government refused to disclose the material and the district court agreed with the government. *Id.* at 999-1000.

The Ninth Circuit reversed the discovery rulings and vacated the conviction, holding that the discovery went to "an issue that [was] central to his defense, because it could spell the difference in a suppression motion of the key physical evidence against him." *Id.* at 1001-02. The Ninth Circuit found that the test for materiality under Fed. R. Crim. P. 16(a)(1)(E) is not whether the requested documents are admissible at trial, but rather whether the discovery may assist the defendant in formulating a defense, including to contesting the admissibility of evidence. *Id.* at 1003. As they stated, "[o]ur system of criminal justice relies on an adversary system to help ensure that justice will be done." *Id.* at 1000. While the government documents may have been sensitive in nature, the defendant's "interest in government materials that are pertinent to his defense takes precedence." *Id.* at 1003; *see also United States v. Budziak*, 697 F.3d 1105, 112-13 (9th Cir. 2012) ("In cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless.").

Argument

The government must be compelled to tender to Mr. Mitrovich the requested discovery as it directly relates to his ability to litigation a motion to suppress. The requested software information will be able to shed light on the capabilities of the software utilized in seizing the IP address including, but not limited to: the ability to involuntarily redirect users from the private "Tor" network to an open Internet connection, the ability to capture of the user's actual IP address, as well as a session identifier to tie the IP address to the activity of a particular TLZ user account, and what other invasive abilities did the software use or have available to otherwise retract information from Mr. Mitrovich's computer.

To that end, the communications between the FBI and QPS/DIA will allow Mr. Mitrovich to establish that the FBI and QPS/DIA were working in concert with one another at the time the IP address was seized. So much so is at least inferred in the government's own reports, noting that it was their identification of TLZ's IP address that ultimately allowed QPS/DIA to seize control of the website. Considering QPS/DIA was not able to use the hyperlink software to redirect users from the "Tor" network to an open Internet connection until they had control of TLZ, it seems to follow that the government was in communications with QPS/DIA regarding TLZ long before the seizure of Mr. Mitrovich's alleged IP address.

The government finds its footing in denying Mr. Mitrovich's request in that he did not have a reasonable expectation of privacy in the IP address because he voluntarily clicked the infected hyperlink on TLZ. This position is presumably

rooted in *United States v. Caira*, where the Seventh Circuit found that the defendant did not have a reasonable expectation of privacy in his IP Address. *See generally*, 833 F.3d 803 (7th Cir. 2016). The Seventh Circuit found that "[b]ecause Caira voluntarily shared his I.P. addresses with Microsoft, he had no reasonable exceptions of privacy in those addresses. So the DEA committed no Fourth Amendment "search" when it subpoenaed that information[.]. *Id*. at 809. Essentially, because *Caira* voluntarily used a Hotmail email account, Microsoft was able to store his IP address in their system, and the information fell within the "third-party doctrine." *Id*. at 806; *citing United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979). Here, however, the IP address was not voluntarily provided to a third-party and is subject to the user's reasonable expectation of privacy in that number.

Under the Fourth Amendment, a "search" occurs when "the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). For an "intrusion into [the] private sphere" to constitute a "search", an individual must "seek[ ] to preserve something as private," and society [must be] prepared to recognize [that privacy expectation] as reasonable." *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018); *quoting Smith*, 442 U.S. at 740.

As this Court previously noted in its Memorandum Opinion and Order in *United States v. Diggs, et at.*, Case No. 18CR185 (Dkt. 78), *Carpenter* explained, *Smith* and *Miller* did not create a bright-line rule: "The third-party doctrine partly

stems from the notion than individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of diminished privacy interest does not mean that the Fourth Amendment falls out of the picture entirely." *Carpenter*, 138 S.Ct. at 2219. The Supreme Court has already found that individuals have a reasonable expectation of privacy in their cell phone, due to the extensive amount of personal information contained therein. *Riley v. California*, 134 S. Ct. 2473 (2014). Indeed, it is reasonable to find that individuals also have a reasonable expectation of privacy in their personal computers, due to the vast amount of personal information they contain. *See United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001); *Gust v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001).

Surely when a typical Internet user browses various websites, he voluntarily provides his IP address to those websites. Such was the case in *Caira*, where the defendant voluntarily used Microsoft's email services. The same is true for the other out-of-circuit cases cited in *Caira*. That triggered the "third-party doctrine" and eliminated any reasonable expectation of privacy an individual had in his IP address, allowing the government to simply subpoena one of the several websites or providers voluntarily visited by a defendant. Taking the governments allegations as true, however, Mr. Mitrovich took additional steps keep his IP address private and secret by using the "Tor" network on the "dark web." This is why the infected hyperlink had to be used on TLZ, because the IP addresses of the users were otherwise unavailable to both the FBI and QPS/DIA.

The Eleventh Circuit recently explained IP addresses and the use of "Tor" networks by users to protect their information:

> We begin with a bit of context. In the normal world of web browsing, an internet service provider assigns an IP address—a unique numerical identifier—to every computer that it provides with internet access. Websites can log IP addresses to keep track of the computers that visit, in essence creating a digital guest book. Internet browsing, therefore, isn't quite as private as most people think—it's actually pretty easy, for instance, for law enforcement to find out who visited what sites, when, and for how long simply by subpoenaing IP-address logs from service providers.
>
> Not so when it comes to the "dark web," the part of the internet "only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable." Blog.OxfordDictionaries.com.[2] "The Onion Router"—usually abbreviated "Tor"—is one such software program. Tor, which was the brainchild of the U.S. Navy but has since been released to the public, works by routing a user's webpage requests through a series of computer servers operated by volunteers around the globe, rendering the user's IP address essentially unidentifiable and untraceable. In the words of the folks who currently administer the "Tor Project," a Massachusetts-based § 501(c)(3) organization responsible for maintaining Tor, you might think of what Tor does as "using a twisty, hard-to-follow route in order to throw off someone who is tailing you—and then periodically erasing your footprints."[3]
>
> As you can imagine, Tor has plenty of legitimate uses—think military and law-enforcement officers carrying out investigations, journalists seeking to maintain anonymity, and ordinary citizens researching embarrassing topics. As you can also imagine, Tor has spawned—and effectively enables—a cache of unsavory sites for black-market trading,

[2] *See also* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1087 (2017) ("The dark web is a private global computer network that enables users to conduct anonymous transactions without revealing any trace of their location.").

[3] *See* Lee Matthews, *What Tor Is, and Why You Should Use It to Protect Your Privacy*, Forbes (Jan. 27, 2017, 2:30 p.m.), https://www.forbes.com/sites/leemathews/2017/01/27/what-is-tor-andwhy-do-people-use-it/#3186d5387d75 (last visited Aug. 27, 2019); *see also* Tor Project, https://2019.www.torproject.org/projects/torbrowser.html.en ("[Tor] prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.") (last visited Aug. 27, 2019).

> child-pornography file-sharing, *1283 and other criminal enterprises. This is so because, in addition to allowing users to access public websites without leaving a trail, Tor also hosts a number of so-called "hidden services," *i.e.*, sites accessible *only* through Tor. You can't just Google a hidden service; rather, a user can access one of these Tor-specific sites only by knowing its exact URL address. Most Tor-site addresses comprise a random jumble of letters and numbers followed by the address ".onion"—in place, say, of ".com" or ".org"—and are shared via message-board postings on the regular internet or by word of mouth.

United States v. Taylor, 935 F.3d 1279, 1282-83 (11th Cir. 2019).

Here, TLZ users who clicked the infected hyperlink were involuntarily redirected to an open Internet network. For obvious reasons, members of TLZ used "Tor" to protect their privacy and it was their voluntary decision to do so. But users such as "cyberguy" never voluntarily left the "Tor" network. Although the users were prompted that by clicking the hyperlink they were be redirected to another website, there was no indication this website would be on the open Internet as opposed to the "dark web" where their privacy interests were secure. The government had to use such misleading tactics to lure unwilling individuals to a network where their information was no longer private and anonymous as they had expected.

Individuals frequenting TLZ would never make an affirmative decision to leave "Tor" and the government knew and understood this. That is the reason that after TLZ was covertly overtaken by investigating agencies, users had to be misled as to where the hyperlinked video was taking them – to a government-controlled website. They were not taken to another website within "Tor" as they excepted, but rather were involuntarily redirected to an open network where their information

was vulnerable. Unlike defendant such a *Caira* who voluntarily used conveyed their IP address information, individuals using "Tor" who are then redirected an open network cannot make a knowing and voluntary decision if they do not know what they are consenting to when clicking the hyperlink. And where an individual's movements and decisions are controlled by the government, in an effort to seize information the individual is taking affirmative steps to keep private; the situation stinks of a Fourth Amendment violation.

There is a significant difference between obtaining an IP address from a third party and obtaining it directly from a defendant's computer. *See Riley*, 134 S. Ct. at 2492-93 (finding a distinction between evidence about phone usage obtained from the phone company and evidence about phone usage obtained directly from the phone itself). "If a defendant writes his IP address on piece of paper and places it in a drawer in his home, there would be no question that law enforcement would need a warrant to access that piece of paper – even accepting that the defendant had no reasonable expectation of privacy in the IP address itself. Here, Defendant[ ] IP address[ ] [was] stored on [his] computer[ ] in [his] home[ ] rather than in a drawer." *United States v. Croghan*, Case No. 15 CR 48 (S.D.Iowa, Sept. 19, 2016).

In light of *Riley*, there is also distinct difference between the government obtained an individual's IP address from websites that they voluntarily visited as opposed to involuntarily redirected users to a network significantly less secure and private that the one they were purposefully using. By redirecting TLZ users from the "Tor" network to an open Internet network, the government was essentially

controlling individuals' movements against their will. "If technology, or a near-future improvement, gives police the power to gather information that is the 'modern-day equivalent' of activity that has been held to be a Fourth Amendment search, the use of that technology is also a search. Orin Kerr, *The Many Revolution of* Carpenter, Harv. J.L. & Tech. (2019); *citing Carpenter*, 138 S. Ct. at 2222 (calling Justice Kennedy's "modern-day equivalent" discussion a "sensible exception") (Kennedy, J., dissenting).

Mr. Mitrovich certainly has a Fourth Amendment right in information stored inside his computer unless he voluntarily shares that information. By using "Tor", the IP address was not voluntarily shared with the website that were visited on the network. This absence of voluntarily sharing this information is exactly what led the government to surreptitiously obtained the information. As such, the issue presented here is not whether the information (IP address) that the government obtained was private, but it is the way that they obtained the information that made the act a search, not the information itself. *See Arizona v. Hicks*, 480 U.S. 321, 325 (1987) ("A search is a search, even if it happens to disclose nothing but the bottom of a turntable."). "What matters is how the government obtained the information, not whether it could have obtained the information some other way that would not be a search."[4]

[4] *See* Orin Kerr, *Remotely accessing an IP address inside a target computer is a search*, The Washington Post (Oct. 7, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/07/remotely-accessing-an-ip-address-inside-a-target-computer-is-a-search/ (last accessed Dec. 3, 2019).

The issue presented here is certainly a novel issue, at least as it pertains to the Seventh Circuit. In other cases, some of which are cited in this motion, the government obtained a warrant to access an individuals IP address by using a "Network Investigative Technique" ("NIT"). *See, e.g., United States v. Michaud*, 2016 WL 337263 (W.D. Wash May 25, 2016); *United States v. Tippens*, 773 Fed.Appx. 383 (9th Cir. 2009). Here, there was no warrant. By granting this motion to compel, this Court will allow Mr. Mitrovich to fully understand the already-apparent invasiveness of the software used to redirect "cyberguy" from the "Tor" network to an open Internet network. Furthermore, it will allow him to understand the relationship between FBI and QPS/DIA. Their communications, just based on their own reports, show that there is a high probability that they were working together. It is certainly a strange situation if the FBI gives the QPS/DIA the IP address for them seize control of TLZ and then does not have any involvement in the sting operation set up to identify members such as "cyberguy".

At this point, Mr. Mitrovich is not asking this Court to rule on the merits for a potential motion to suppress, but he has certainly met the *prima facie* standard to require the government to turn over the requested information. "At the [Fourth Amendment's] very core stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion." *Silverman v. United States*, 365 U.S. 505, 511 (1961). "This protection, through previously tied to common-law trespass, now encompasses searches of the home made possible by ever-more sophisticated technology. Any other rule would "erode the privacy

guaranteed by the Fourth Amendment." *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 525-26 (7th Cir. 2018) (internal citations omitted). This Court must allow Mr. Mitrovich to obtain the requested information from the government in order to properly investigate and research his ability to litigate a motion to suppress and protect his rights of due process.

Conclusion

Wherefore, defendant Deny Mitrovich respectfully requests this Honorable Court to grant the instant motion and enter and order compelling the government to comply with their discovery obligations and turn over all documents and records requested, as discussed herein.

Respectfully submitted,

/s Vadim A. Glozman
Attorney For The Defendant

Vadim A. Glozman
VADIM A. GLOZMAN LTD.
Attorney at Law
53 W. Jackson Blvd., Suite 1410
Chicago, IL 60604
(312) 726-9015

CERTIFICATE OF SERVICE

I, Vadim A. Glozman, an attorney for Defendant Deny Mitrovich, hereby certify that on this, the 3rd day of December, 2019, I filed the above-described document on the CM-ECF system of the United States District Court for the Northern District of Illinois, which constitutes service of the same.

Respectfully submitted,

/s/ Vadim A. Glozman

53 W. Jackson Blvd., Suite 1410
Chicago, IL 60604
(312) 726-9015